(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 488 720 A1**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **91310998.9**

(51) Int. Cl.[5] : **G06K 19/06,** G07F 7/10

(22) Date of filing : **28.11.91**

(30) Priority : **29.11.90 JP 325263/90**

(43) Date of publication of application :
03.06.92 Bulletin 92/23

(84) Designated Contracting States :
DE FR

(71) Applicant : **KABUSHIKI KAISHA TOSHIBA**
72, Horikawa-Cho Saiwai-ku
Kawasaki-shi Kanagawa-ken (JP)
(71) Applicant : **TOSHIBA INTELLIGENT TECHNOLOGY LTD.**
70, Yanagi-cho Saiwai-ku
Kawasaki-shi Kanagawa-ken (JP)

(72) Inventor : **Kuriyama, Ryouichi, c/o Intellectual Property Div.**
Toshiba Corporation, 1-1-1 Shibaura
Minato-ku (JP)

(74) Representative : **Shindler, Nigel et al**
BATCHELLOR, KIRK & CO. 2 Pear Tree Court
Farringdon Road
London EC1R 0DS (GB)

(54) A portable electronic device and a method for processing data therefor.

(57) A portable electronic device contains a memory having first, second and third memory areas and a CPU. A plurality of identification number data are stored in the first memory area of the memory. The portable electronic device receives identification number data and instruction data from an external device. The CPU verifies the identification number data received by this device by reference to the identification number data stored in the first memory area of the memory and stores verification results in the second memory area of the memory. The portable electronic device also receives instruction data from the external device. Control data corresponds to the instruction data are stored in the third memory area and represent a plurality of identifiers each indicating whether identification number verification is required and further indicates whether complete or partial identification number verification is required. The CPU refers to the verification results stored in the second memory area of the memory in accordance with the control data stored in the third memory area of the memory after the instruction data has been received and executes the instruction data in response to the verification results.

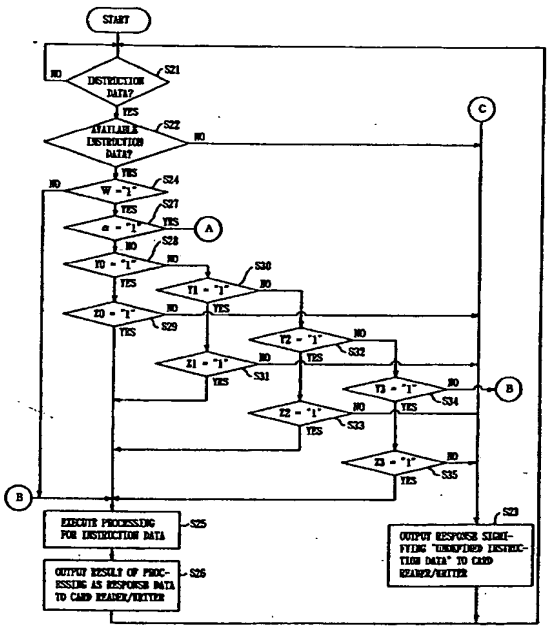

FIG. 10A

EP 0 488 720 A1

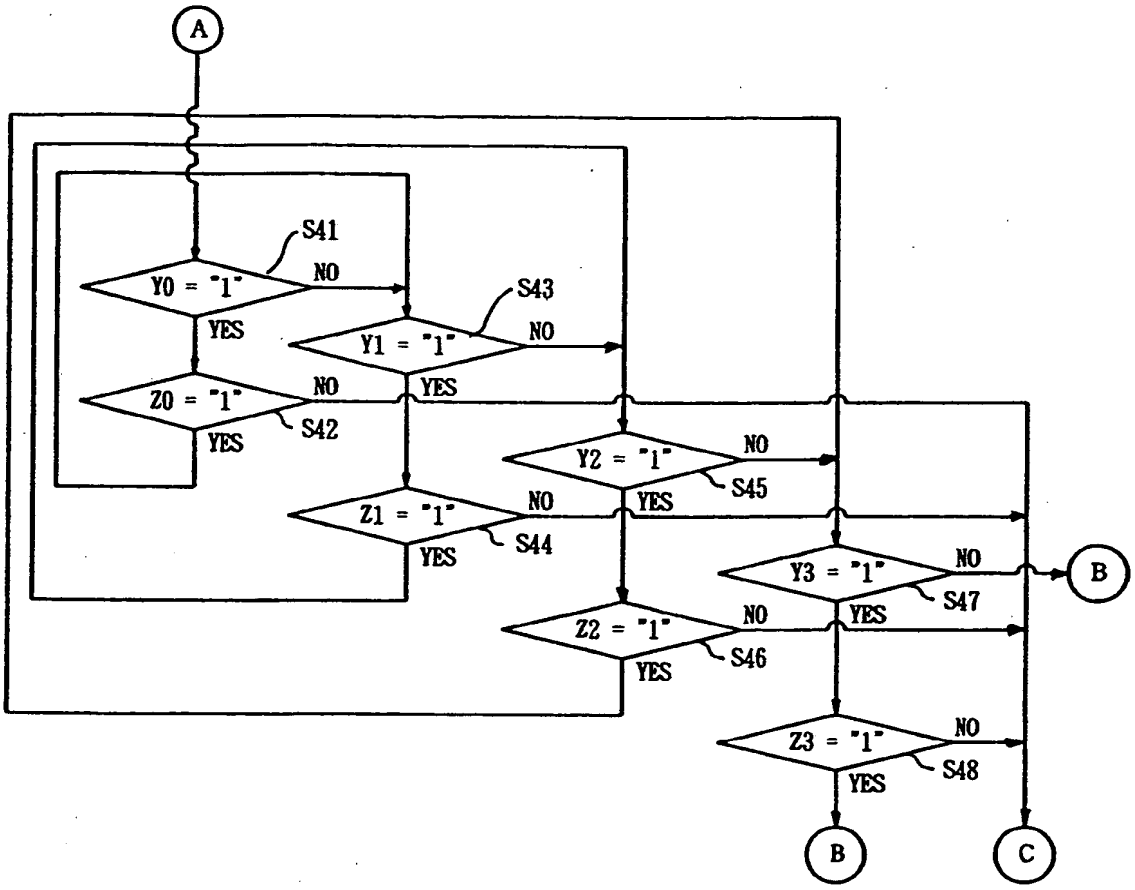
A
S41
Y0 = "1"
NO
YES
S43
Y1 = "1"
NO
YES
Z0 = "1"
NO
YES
S42
Y2 = "1"
NO
S45
YES
Z1 = "1"
NO
YES
S44
Y3 = "1"
NO
S47
B
YES
Z2 = "1"
NO
S46
YES
Z3 = "1"
NO
S48
YES
B
C

FIG. 10B

The present invention relates to a portable electronic device such as an IC card and a method for processing data therefor.

Recently ID cards have been developed as new portable data memory media in which IC chips having control elements such as, for instance non-volatile data memories and CPUs are housed. This type of IC card selectively executes the input and output of required data by the control element accessing the data memory in response to instruction data entered from outside. In this case, the data memory is divided into a plurality of data areas, and it is designed selectively to access the subject area.

In a prior art IC card, whether or not verification of an ID (identification) number is required for each of the plurality of data areas is set for the data memory data area by data area, or a key is applied for setting the ID number verification state for the card manufacturer, the card-issuer and the card-holder. For instance, in the case of a relevant data area being only available for the card-issuer, if the card-issuer's ID number is verified and instruction data is inputted, processing for that instruction data is executed. However, when instruction data is entered by someone other than the card-issuer, response data to the effect that execution conditions are not in order is generated, and processing of the instruction data will not be executed. That is, if instruction data is inputted by someone other than the card-issuer, for instance, the card-holder, response data to the effect that execution conditions are not in order is generated. However it is possible that the card-holder will guess that instruction data can be executed when instruction data is entered by the card-manufacturer or card-issuer. Thus, if the card-holder is unlawfully aware of the card-issuer's or card-manufacturer's ID number, there is danger that the execution of instruction data will be performed by entering instruction data based on the card-issuer's or card-manufacturer's ID number which is fraudulently entered by the card-holder or a third party.

In the case of instruction data which is undefined or not available being entered by, for instance, the card-holder, response data signifying 'undefined instruction data' is generated. However, it is possible that the card holder will guess that instruction data other than the ID number is undefined. Thus, there is a danger that defined or available instruction data can be guessed by entering data at random (i.e. until a negative response is not produced), that is, there is the possibility of the available instruction data becoming identified, and therefore there is a problem of poor security.

Accordingly the present invention seeks to provide a portable electronic device in which security is improved without available instruction data becoming easily identified.

The present invention also seeks to provide a method for processing data for a portable electronic device in which security is improved without available instruction data becoming easily identified.

According to the present invention there is provided a portable electronic device comprising first memory means for storing a plurality of identification number data, means for receiving a plurality of instruction data including identification number verifying instructions from an external device, means for verifying the identification number data received by the receiving means by reference to the identification number data stored in the first memory means when the receiving means receives identification number data including identification number verifying instructions, second memory means for storing verification results, third memory means for storing control data corresponding to the instruction data and representing a plurality of identifiers each indicating whether identification number verification is required and further indicating whether complete or partial identification number verification is required, means for referring to the verification results stored in the second memory means in accordance with the control data stored in the third memory means after the instruction data other than the identification number verifying instruction data has been received by the receiving means, and means for executing the instruction data in response to the verification results.

Further, according to the present invention there is provided a method for processing data by a portable electronic device with a memory having first to third memory areas, the method comprising the steps of storing a plurality of identification number data in the first area of the memory; receiving identification number data from an external device; verifying the identification number data received in the receiving step by reference to the identification number data stored in the first memory area of the memory; storing verification results in the second area of the memory; receiving instruction data from the external device; storing, in the third memory area of the memory, control data corresponding to the instruction data and representing a plurality of identifiers each indicating whether identification number verification is required and further indicating whether complete or partial identification number verifications is required; referring to the verification results stored in the second memory area of the memory in accordance with the control data stored in the third memory area of the memory after the instruction data has been received; and executing the instruction data in response to the verification results.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a block diagram showing the construction of an IC card handling system to be applied to a method for processing data for a port-

able electronic device of the present invention;
FIGURE 2 is a block diagram showing the composition of an IC card of the present invention;
FIGURE 3 is a diagram showing the composition of the program memory in the IC card;
FIGURE 4 is a diagram showing the composition of the data memory in the IC card;
FIGURE 5 is a diagram showing a memory example of lead addresses and control information for functional programs stored corresponding to function codes;
FIGURE 6 is a diagram showing the control data in detail;
FIGURE 7 is a diagram showing a memory example of identification numbers data;
FIGURE 8 is a diagram showing data representing the result of ID collation in detail;
FIGURE 9 is a flow-chart illustrating the ID verifying operation; and
FIGURES 10A and 10B are flow-charts illustrating the processing operation.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to the accompanying drawings, a detailed description will subsequently be given of the preferred embodiment of the present invention.

FIGURE 1 shows a block diagram of a card handling system in which an IC card is applied as the portable electronic device. The system is constructed by making IC card 1 connectable to CPU 3 functioning as a control section via card reader/writer 2. Keyboard 4, CRT display unit 5, printer 6 and floppy disk drive unit 7 are connected to CPU 3.

FIGURE 2 shows a block diagram of IC card 1. IC card 1 is composed of CPU 11 as a control element; non-volatile data memory 12, in which the memory content is erasable, as the data memory unit; program memory 13 as the program memory unit, and contact unit 14 for enabling electrical contact with card reader/writer 2. Of these, the parts within the broken outline (CPU 11, data memory 12 and program memory 13) are contained in one IC chip which is embedded in the main body of the IC card. Program memory 13 is composed of, for instance, a mask ROM. As shown in FIGURE 3, program memory 13 stores the control program for CPU 11 which provides functional programs which respond to a plurality of instruction data. Data memory 12 is used for storing various types of data, and is composed of, for instance, an EEPROM.

As shown in FIGURE 4, data memory 12 is divided and defined into a plurality of areas, and each area is allotted an area number [00, 01, 02,..]. Of these, in AREA [00] 12a, the respective area lead addresses and area sizes (the numbers of bytes which compose the areas) of all areas are stored corresponding to the area numbers. For instance, this operates in such a way that lead address A03 and area size S03 bytes correspond to AREA [03] 12d. Also, as shown in FIGURE 5, in AREA [01] 12b, the lead address and control data of each functional program is stored corresponding to a function code. For instance, this operates in such a way that the lead address of the program which executes function code [B] is bbb, and the corresponding control data is b1. Moreover, as shown in FIGURE 7, a plurality of identification (hereinafter referred to as ID) number data X0-X3 is stored in AREA [02] 12c. These ID number data X0-X3 are used for verification of ID numbers. For instance, these are ID number data for the card-manufacturer, the card-issuer, the card-holder, etc. AREA [03] 12d, AREA [04] 12e and succeeding areas are respectively data areas.

FIGURE 6 shows the detail of the control data, which are stored in memory area 12bb of AREA [01] 12b, mentioned above. This is composed of identifiers Y0-Y3, W and α. That is, identifiers Y0-Y3 correspond to the above ID number data X0-X3 and indicate whether or not verification of these ID numbers data is required. For instance "1" represents 'required' and "0" represents 'not required'. For instance, if identifier Y0 is "1", this represents that verification of ID number data by ID number data X0 is required. Also, identifier W represents whether checking of identifiers Y0-Y3 is required. For instance "1" represents 'required' and "0" represents 'not required'.

In the combination of identifiers Y0-Y3, identifier a establishes whether all of the ID number verifications or only part of the ID number verifications is required. For instance, "1" represents 'all required' and "0" represents 'part only required'.

FIGURE 8 shows the information which represent the result of the verification of ID numbers, and is composed of identifiers Z0-Z3. That is, identifiers Z0-Z3 correspond to respective ID number data X0-X3, and represent the verification results of these. For instance, "1" represents 'verification agreed' and "0" represents 'verification disagreed'. For instance, if identifier Z0 is "1", this represents that the result of ID number verification by ID number data X0 is 'verification agreed'. Also, this data, that is identifiers Z0-Z3, is stored in memory area 11a in the RAM which is housed in CPU 11.

The operation in this type of construction will now be described. First, the ID number verification operation is described with reference to the flow-chart shown in FIGURE 9. In the regular state, IC card 1 is in the ready state for instruction data from card reader/writer 2. In this state, when instruction data from card reader/writer 2 is entered (step S1), CPU 11 judges whether or not this is ID number verifying instruction data (step S2). If it is ID number verifying instruction data, the ID number data to be collated (shown as PIN (Personal Identification Number) in the

flow-chart) attributed to this instruction data is sequentially collated with each ID number data X0-X3 stored in area [02] of data memory 12 (steps S3, S5, S7 and S9). If there is ID number data which agrees as the result of this verification, CPU 11 sets the identifier (Z0-Z3) in the RAM which corresponds to the ID number data to "1" (steps S4, S6, S8 and S10). For instance, if PIN agrees with ID number data X0, identifier Z0 is set to "1" (step S4), and if PIN agrees with ID number data X3, identifier Z3 is set to "1" (step S10). Then, CPU 11 generates response data signifying 'verification agreed' to card reader/writer 2 (step S11), and returns to the ready for instruction data state. If, as the result of the above verification, there is no agreement with any of ID number data X0-X3, CPU 11 generates response data signifying 'verification disagreed' to card reader/writer 2 (step S12), and returns to the ready for instruction data state.

The processing operation based on the instruction data will now be described with reference to the flow-charts shown in FIGURES 10A and 10B. In the regular state, IC card 1 is in the ready state for instruction data from card reader/writer 2. In this state, when instruction data from card reader/writer 2 is entered (step S21), CPU 11 judges whether or not this is available instruction data (step S22). If it is not available instruction data, CPU 11 generates response data signifying 'undefined instruction data' to card reader/writer 2 (step S23) and returns to the ready for instruction data state. If the data is available instruction data, CPU 11 finds the function code attributed to the instruction data from area [01] of data memory 12. Then, CPU 11 refers to the identifier W of the stored control information corresponding to that function code and judges whether W is "1" or not (step S24). If identifier W is not "1", checking of identifiers Y0-Y3 is not required (that is, ID number verification is not required). Thus, CPU 11 executes processing by a functional program corresponding to the relevant instruction data (step S25). That is, CPU 11 recognises the lead address of the functional program stored corresponding to the function code found from area [01] of data memory 12 and steps to that functional program. Then, processing is executed by that functional program, and the processing result is outputted to card reader/writer 2 as response data (step S26), and it returns to the ready for instruction data state.

If identifier W is "1" and the corresponding identifier a is not "1" (step S27), CPU 11 refers to the corresponding control data identifier Y0 (step S28). If identifier Y0 is "1", CPU 11 refers to identifier Z0 of the data representing the result of the ID number verification (step S29), and judges whether this is "1" or not. If Z0 is "1", ID number verification has already been executed, and a verification agreed result has been obtained. In step S29, if Z0 is not "1", since a verification agreed result has not been obtained, response data signifying 'undefined instruction data' is outputted (step S23), and it enters the ready for instruction data state.

In step S28, if identifier Y0 is not "1", CPU 11 refers to control data identifier Y1 (step S30), and if this is "1", CPU 11 refers to identifier Z1 representing the result of the ID number verification and judges whether this is "1" or not (step S31). If Z1 is "1", ID number verification has already been executed and a verification agreed result has been obtained. If Z1 is not "1", since a verification agreed result has not been obtained, response data signifying 'undefined instruction data' is generated (step S23), and it enters the ready for instruction data state.

In step S30, if Y1 is not "1", CPU 11 refers to control data identifier Y2 (step S32), and if this is "1", CPU 11 refers to identifier Z2 and judges whether this is "1", or not (step S33). If Z2 is "1", ID number verification has already been executed and a verification agreed result has been obtained. If Z2 is not "1", since a verification agreed result has not been obtained, response data signifying 'undefined instruction data' is generated (step S23), and it enters the ready for instruction data state.

In step S32, if Y2 is not "1", CPU 11 refers to control data identifier Y3 (step S34), and if this is "1", CPU 11 refers to identifier Z3 and judges whether this is "1", or not (step S35). If Z3 is "1", ID number verification has already been executed and a verification agreed result has been obtained. If Z3 is not "1", since a verification agreed result has not been obtained, response data signifying 'undefined instruction data' is generated(step S23), and it enters the ready for instruction data state.

In step S34, if Y3 is not "1", the flow steps to step S25 as the ID number verification is not required. That is, CPU 11 executes processing by a functional program corresponding to the relevant instruction data (step S25).

In step S27, if identifier α is "1", as shown in FIGURE 10B, CPU 11 refers to the corresponding control data identifiers Y0-Y3 (steps S41, S43, S45 and S47) and finds an identifier which is "1". If CPU 11 finds an identifier which is "1", CPU 11 refers to the identifier (Z0-Z3) of the information representing the result of ID number verification corresponding to that identifier and judges whether it is "1", or not (steps S42, S44, S46 and S48). If each of Z0-Z3 is "1", ID number verification has already been executed and a 'verification agreed' result has been obtained. Therefore, CPU 11 executes processing by the functional program corresponding to the relevant instruction data as described above. If one of Z0-Z3 is not "1", either ID number verification has not been executed or, even if ID number verification has been executed, a 'verification disagreed' result has been obtained. Therefore, CPU 11 does not execute processing, and generates response data signifying 'undefined instruction data' to

card reader/writer 2. It then returns to the ready for instruction data state.

As described above, whether or not ID number verification is required for response to the available instruction data is set. Also, a key is applied to the available instruction data by setting the ID number verification state for the card-manufacturer, the card-issuer and the card-holder. Processing for the instruction data can be selectively executed by judging whether or not the ID number verification result has responded to the instruction data. Also, in the case of unavailable instruction data or the ID number verification result being negative, response data signifying 'undefined instruction data' is generated. By this means, available instruction data do not easily become identified through the response data, and security is improved by judging the combination of the verification results of the card-manufacturer's, card-issuer's and card-holder's IDs.

In the above embodiment, an IC card has been shown as an example of a portable electronic device. However, the present invention is not limited to a card-shaped device. For instance, it may be applied to block-shaped or pencil-shaped devices. Accordingly, it should be understood that the scope of the invention is limited only by the appended claims.

Claims

1. A portable electronic device comprising:

first memory means for storing a plurality of identification number data;

means for receiving a plurality of instruction data including identification number verifying instruction data from an external device;

means for verifying the identification number data received by the receiving means by reference to the identification number data stored in the first memory means, when the receiving means receives the identification number data and the identification number verifying instruction data;

second memory means for storing verification results;

third memory means for storing control data corresponding to the instruction data and representing a plurality of identifiers each indicating whether identification number verification is required and further indicating whether complete or partial identification number verification is required;

means for referring to the verification results stored in the second memory means in accordance with the control data stored in the third memory means after the instruction data excepting the identification number verifying instructions data has been received by the receiving means; and

means for executing the instruction data in response to the verification results.

2. A device according to claim 1, wherein the identifiers include a first identifier (Y0-Y3) designating which of the identification number data should be verified from among the entered identification number data, and a second identifier (a) indicating whether complete or partial identification number verification is required in respect of the designated identification number data designated by the first identifiers (Y0-Y3) is required.

3. A device according to claim 2, wherein the referring means refers to the verification results of the identification number data should be verified.

4. A device according to claim 1, wherein the first, second and third memory means are contained in one data memory element.

5. A device according to claim 1, wherein the means for referring and means for verifying comprise a CPU contained in the portable electronic device.

6. A method for processing data by a portable electronic device with a memory having first to third memory areas, the method comprising the steps of:

storing a plurality of identification number data in the first area of the memory;

receiving identification number data from an external device;

verifying the identification number data received in the receiving step by reference to the identification number data stored in the first memory area of the memory;

storing verification results in the second area of the memory;

receiving instruction data from the external device;

storing, in the third memory area of the memory, control data corresponding to the instruction data and representing a plurality of identifiers each indicating whether identification number verification is required and further indicating whether complete or partial identification number verifications is required;

referring to the verification results stored in the second memory area of the memory in accordance with the control data stored in the third memory area of the memory after the instruction data has been received; and

executing the instruction data in response to the verification results.

7. A method for processing data by a portable elec-

tronic device with a memory having first to third memory areas, the method comprising the steps of:

storing a plurality of identification number data in the first area of the memory;

receiving identification number data and identification number verifying instruction data;

verifying the identification number data received in the receiving step with the identification number data stored in the first memory area of the memory when the identification number data and the identification number verifying instruction data has been received;

storing verification results in the second memory area of the memory for every identification number verifying instruction data;

receiving instruction data excepting the identification number verifying instruction data;

storing, in the third memory area of the memory, a first identifier (W) indicating whether identification number verification is required with corresponding to each of the instruction data excepting the identification number verifying instruction data, a second identifiers (Y0-Y3) designating the identification number data should be verified from among the plurality of identification number data stored in the first area of the memory, and a third identifier (α) indicating whether complete or partial identification number verifications of the identification number data designated by the second identifiers (Y0-Y3) is required;

referring to the verification results of the identification number data should be verified when the identification number verification is required based on the first to third identifiers stored in the third memory area of the memory after the instruction data excepting the identification number verifying instruction data has been received; and

executing the instruction data excepting the identification number verifying instruction data when only the identification number data has been verified in the referring step.

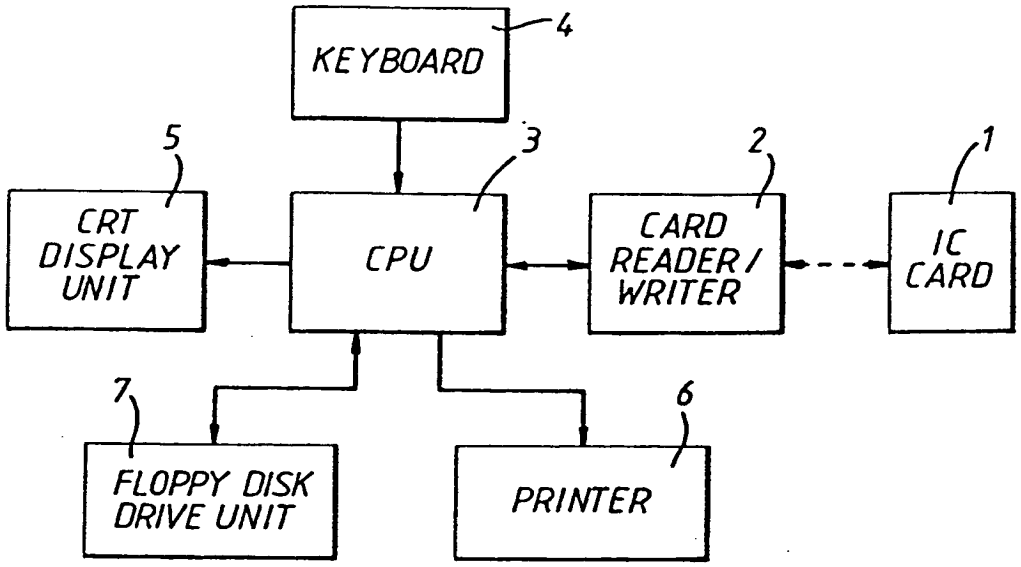
KEYBOARD
4
5
3
2
1
CRT DISPLAY UNIT
CPU
CARD READER / WRITER
IC CARD
7
6
FLOPPY DISK DRIVE UNIT
PRINTER

FIG. 1

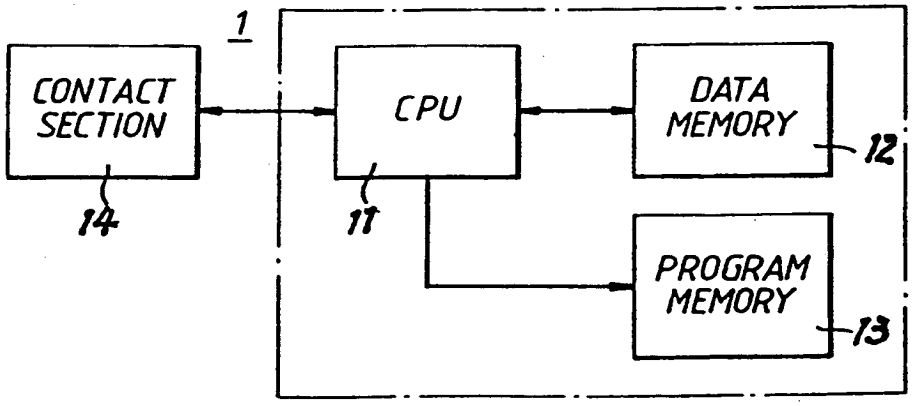
1
CONTACT SECTION
CPU
DATA MEMORY
12
14
11
PROGRAM MEMORY
13

FIG. 2

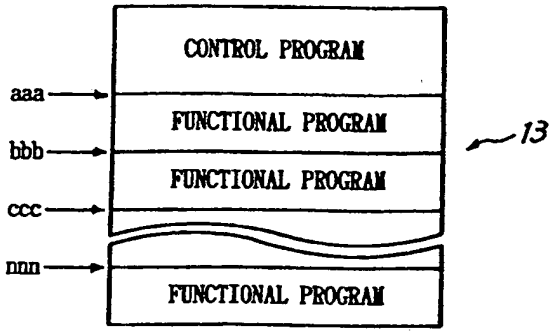
CONTROL PROGRAM
aaa
FUNCTIONAL PROGRAM
bbb
FUNCTIONAL PROGRAM
ccc
nnn
FUNCTIONAL PROGRAM
13

FIG. 3

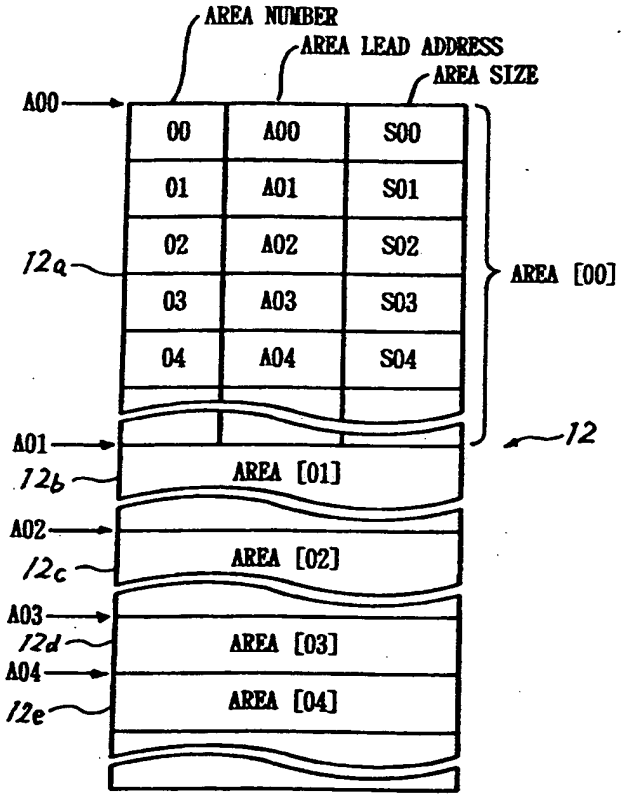
AREA NUMBER
AREA LEAD ADDRESS
AREA SIZE
A00
00 A00 S00
01 A01 S01
02 A02 S02
03 A03 S03
04 A04 S04
12a
AREA [00]
12
A01
AREA [01]
12b
A02
AREA [02]
12c
A03
AREA [03]
12d
A04
AREA [04]
12e

FIG. 4

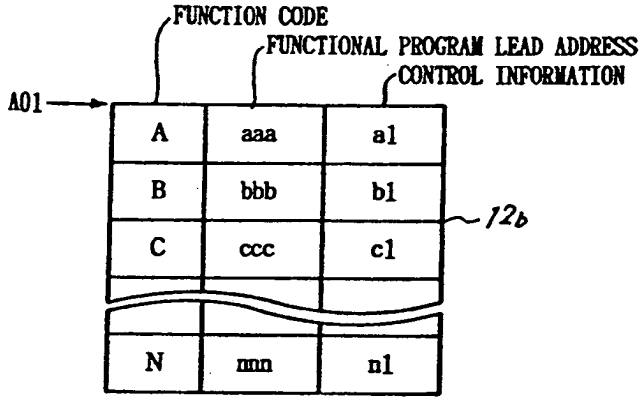

FIG. 5

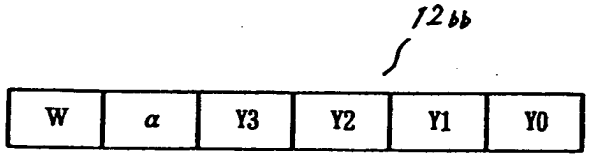

FIG. 6

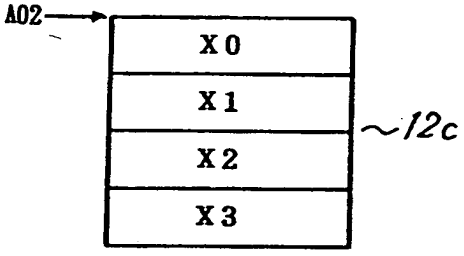

FIG. 7

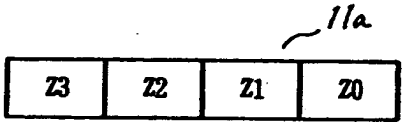

FIG. 8

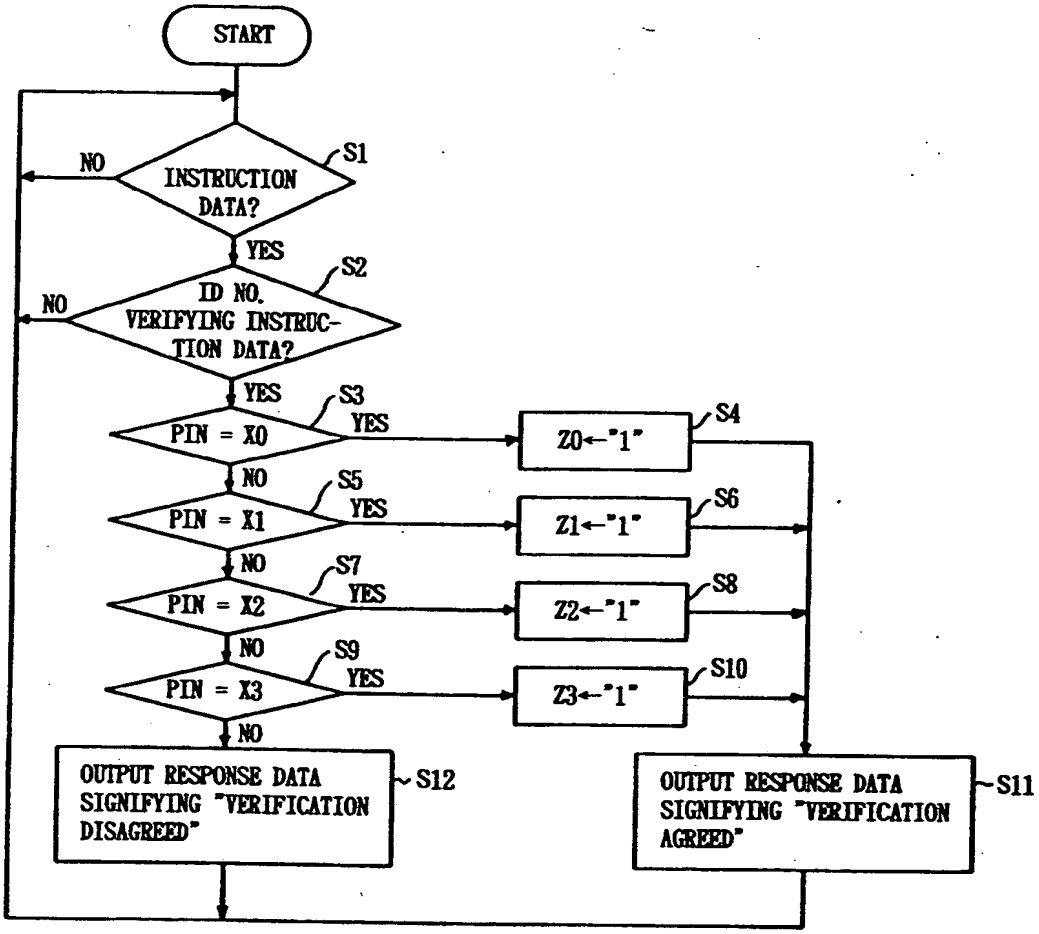
START
S1
INSTRUCTION DATA?
NO
YES
S2
ID NO. VERIFYING INSTRUCTION DATA?
NO
YES
S3
PIN = X0
YES
S4
Z0←"1"
NO
S5
PIN = X1
YES
S6
Z1←"1"
NO
S7
PIN = X2
YES
S8
Z2←"1"
NO
S9
PIN = X3
YES
S10
Z3←"1"
NO
OUTPUT RESPONSE DATA SIGNIFYING "VERIFICATION DISAGREED"
S12
OUTPUT RESPONSE DATA SIGNIFYING "VERIFICATION AGREED"
S11

FIG. 9

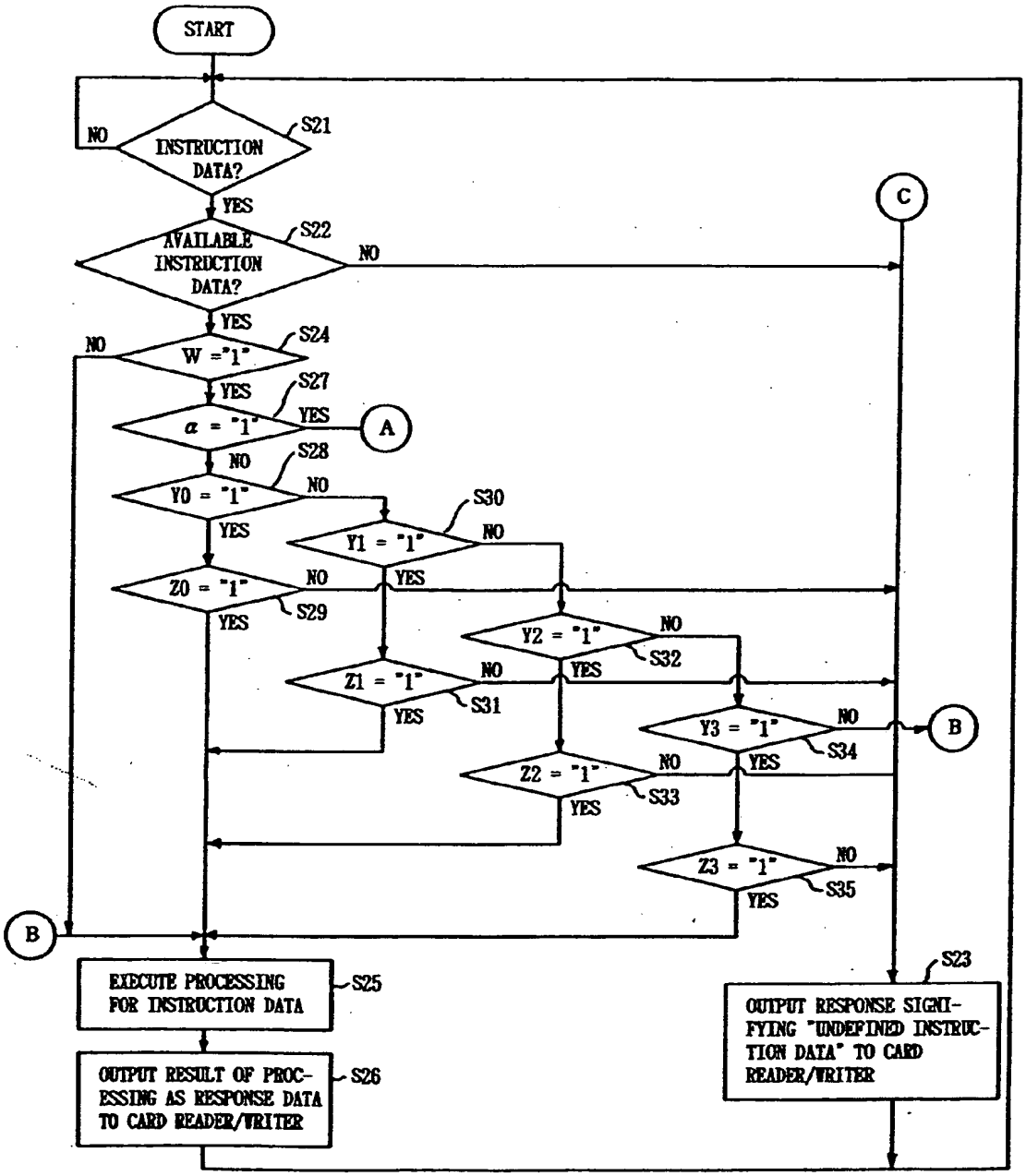
START
INSTRUCTION DATA?
S21
NO
YES
AVAILABLE INSTRUCTION DATA?
S22
NO
YES
W ="1"
S24
NO
YES
α = "1"
S27
YES
A
NO
Y0 = "1"
S28
NO
YES
Y1 = "1"
S30
NO
YES
Z0 = "1"
NO
S29
YES
Y2 = "1"
NO
S32
YES
Z1 = "1"
NO
S31
YES
Y3 = "1"
NO
S34
YES
B
Z2 = "1"
NO
S33
YES
Z3 = "1"
NO
S35
YES
C
B
EXECUTE PROCESSING FOR INSTRUCTION DATA
S25
OUTPUT RESULT OF PROCESSING AS RESPONSE DATA TO CARD READER/WRITER
S26
S23
OUTPUT RESPONSE SIGNIFYING "UNDEFINED INSTRUCTION DATA" TO CARD READER/WRITER

FIG. 10A

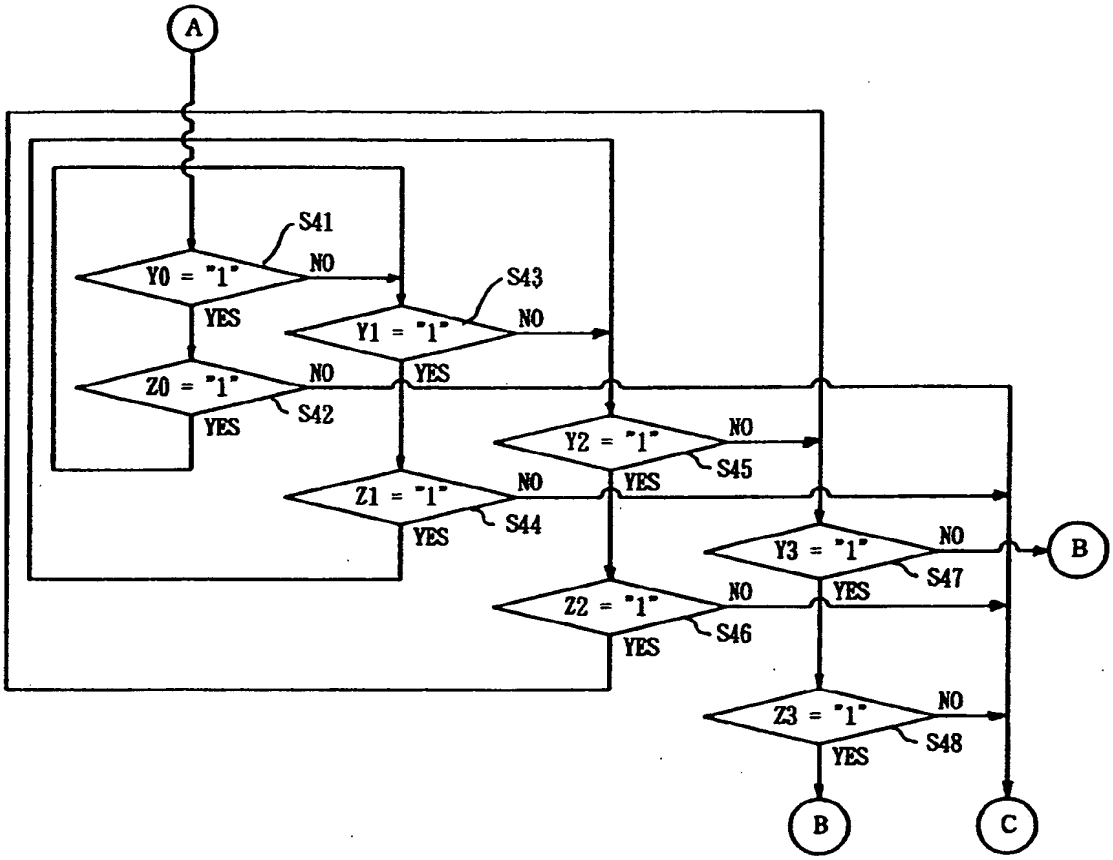
A
S41
Y0 = "1"
NO
YES
S43
Y1 = "1"
NO
YES
Z0 = "1"
NO
YES
S42
Y2 = "1"
NO
S45
YES
Z1 = "1"
NO
YES
S44
Y3 = "1"
NO
S47
B
YES
Z2 = "1"
NO
S46
YES
Z3 = "1"
NO
S48
YES
B
C

FIG. 10B

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 91 31 0998

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
A	EP-A-0 299 826 (SCHLUMBERGER INDUSTRIES) * abstract; claims 1-4 * * column 1, line 1 - column 3, line 60 *	1,4-7	G06K19/06 G07F7/10
A	FR-A-2 635 893 (KABUSHIKI KAISHA TOSHIBA) * abstract; claims 1-5 * * page 1, line 1 - page 4, line 5 *	1,4,6-7	
A	EP-A-0 286 094 (CASIO COMPUTER COMPANY LTD) * abstract; claims 1-15 * * column 1, line 5 - column 2, line 29 *	1,4-7	
A	EP-A-0 291 834 (OKI ELECTRIC INDUSTRY COMPANY) * abstract; claims 1-3 * * column 1, line 5 - line 46 *	1,6-7	
A	FR-A-2 503 423 (FLONIC SA) * page 3, line 1 - page 5, line 12; claim 1 *	1,6-7	

TECHNICAL FIELDS SEARCHED (Int. Cl.5)

G06K
G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	06 MARCH 1992	BEAUCE G.Y.G.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)